WHAT IS CLAIMED IS:

1. A method of recording information on an information recording medium, comprising:

preparing an information recording medium having a first read-only area recording a specified key management information, a second read-only area recording compressed data comprising said key management information compressed with a specified function according to a recording system different from that for said first read-only area, and a writable area for recording, in a writable manner, encrypted content data resulting from encryption based on said key management information;

reading key management information from said first read-only area on said prepared information recording medium and converting said key management information to compressed data by using a specified function;

reading compressed data from said second read-only area and comparing this compressed data with the compressed data obtained at said conversion;

when both match as a result of said comparison, generating a content key from said key management information by using its own device key; and

encrypting input content data by using said generated content key and recording the obtained encrypted content data on said writable area.

2. A method of producing an information recording

medium, comprising:

preparing an information recording medium having a first read-only area recording a specified key management information, a second read-only area recording compressed data comprising said key management information compressed with a specified function according to a recording system different from that for said first read-only area, and a writable area for recording, in a writable manner, encrypted content data resulting from encryption based on said key management information;

reading key management information from said first read-only area on said prepared information recording medium and converting said key management information to compressed data by using a specified function;

reading compressed data from said second read-only area and comparing this compressed data with the compressed data obtained at said conversion;

when both match as a result of said comparison, generating a content key from said key management information by using its own device key; and

encrypting input content data by using said generated content key and recording the obtained encrypted content data on said writable area.

3. A method of playing information from an information recording medium, comprising:

preparing an information recording medium having a first read-only area recording a specified key management information, a second read-only area recording compressed data comprising said key management information compressed with a specified function according to a recording system different from that for said first read-only area, and a writable area recording, in a writable manner, encrypted content data resulting from encryption based on said key management information;

reading key management information from said first read-only area on said information recording medium and converting said key management information to compressed data by using a specified function;

reading compressed data from said second read-only area and comparing this compressed data with the compressed data obtained at said conversion;

when both match as a result of said comparison, generating a content key from said key management information by using its own device key; and

reading said encrypted content data from said writable area, decrypting said encrypted content data by using said generated content key, and outputting obtained content data.

4. An information recording medium comprising:

a first read-only area recording specified key management information;

a second read-only area recording compressed data comprising said key management information compressed with a specified function according to a recording system different from that for said first read-only area; and

a writable area for recording, in a writable manner, encrypted content data resulting from encryption based on said key management information.

5. The information recording medium according to claim 4, wherein

said first read-only area is formed between said second read-only area and said writable area.

6. The recording apparatus for recording information on the information recording medium described in claim 4, comprising:

a compression circuit configured to convert key management information read from a first read-only area on said information recording medium to compressed data by using a specified function;

a comparison circuit configured to compare compressed data read from a second read-only area on said information recording medium with compressed data obtained in said compression circuit;

a key generation circuit configured to generate a content key from said key management information by using its own device key when a match is found as a result of comparison by said comparison circuit; and

an encryption recording circuit configured to encrypt input content data by using a content key generated in said key generation circuit and record obtained encrypted content data onto said writable area.

7. The playback apparatus for playing information from the information recording medium described in claim 4, comprising:

a compression circuit configured to convert key management information read from a first read-only area on said information recording medium to compressed data by using a specified function;

a comparison circuit configured to compare compressed data read from a second read-only area on said information recording medium with compressed data obtained in said compression circuit;

a key generation circuit configured to generate a content key from said key management information by using its own device key when a match is found as a result of comparison by said comparison circuit; and

a decryption circuit configured to decrypt encrypted content data read from a writable area on said information recording medium by using a content key generated in said key generation circuit and output obtained content data.

8. An information recording medium comprising:

a first read-only area recording specified key management information, wherein said key management information, after it is read, is used as compressed data converted with a specified function and is compared to compressed data in said second read-only area.

a second read-only area recording compressed data comprising said key management information compressed with a specified function according to a recording system different from that for said first read-only area; and

a writable area for recording, in a writable manner, encrypted data to be recorded based on said key management information when said comparison results in a match.

9. A method of recording information on an information recording medium, comprising:

preparing an information recording medium having a writable area for recording, in a writable manner, specified key management information and encrypted content data and a read-only area recording compressed data comprising said key management information compressed with a specified function according to a recording system different from that for said writable area;

reading key management information from said writable area on said prepared information recording medium and converting said key management information to compressed data by using a specified function;

reading compressed data from said read-only area and comparing this compressed data with the compressed data obtained at said conversion;

when both match as a result of said comparison, generating a content key from key management information by using its own device key; and

encrypting input content data by using said generated content key and recording the obtained encrypted content data on said writable area.

10. A method of producing an information recording medium, comprising:

preparing an information recording medium having a writable area for recording, in a writable manner, specified key management information and encrypted content data and a read-only area recording compressed data comprising said key management information compressed with a specified function according to a recording system different from that for said writable area;

reading key management information from said writable area on said prepared information recording medium and converting said key management information to compressed data by using a specified function;

reading compressed data from said read-only area and comparing this compressed data with the compressed data obtained at said conversion;

when both match as a result of said comparison, generating a content key from key management information by using its own device key; and

encrypting input content data by using said generated content key and recording the obtained encrypted content data on said writable area.

11. A method of playing information from an information recording medium, comprising:

preparing an information recording medium having a writable area for recording, in a writable manner, specified key management information and encrypted content data and a read-only area recording compressed data comprising said key management information compressed with a specified function according to a recording system different from that for said writable area;

reading key management information from said writable area on said prepared information recording medium and converting said key management information to compressed data by using a specified function;

reading compressed data from said read-only area and comparing this compressed data with the compressed data obtained at said compression step;

when both match as a result of said comparison, generating a content key from key management information by using its own device key; and

reading said encrypted content data from a writable area on said information recording medium, decrypting said encrypted content data by using said generated content key, and outputting obtained content data.

12. A method of recording information on an information recording medium, comprising:

preparing an information recording medium having a first read-only area recording a specified key management information, a second read-only area recording compressed data comprising said key management information compressed with a specified function according to a recording system different from that for said first read-only area, and a third read-only area capable of only once recording encrypted content data resulting from encryption based on said key management information;

reading key management information from said first read-only area on said prepared information recording medium and converting said key management information to compressed data by using a specified function;

reading compressed data from said second read-only area and comparing this compressed data with the compressed data obtained at said conversion;

when both match as a result of said comparison, generating a content key from said key management information by using its own device key; and

encrypting input content data by using said generated content key and recording the obtained encrypted content data on said third read-only area.

13. A method of producing information recording medium, comprising:

preparing an information recording medium having a first read-only area recording a specified key management information, a second read-only area recording compressed data comprising said key management information compressed with a specified function according to a recording system different from that for said first read-only area, and a third read-only area capable of only once recording encrypted content data resulting from encryption based on said key management information;

reading key management information from said first read-only area on said prepared information recording medium and converting said key management information to compressed data by using a specified function;

reading compressed data from said second read-only area and comparing this compressed data with the compressed data obtained at said conversion;

when both match as a result of said comparison, generating a content key from said key management information by using its own device key; and

encrypting input content data by using said generated content key and recording the obtained encrypted content data on said third read-only area.

14. A method of playing information from an information recording medium, comprising:

preparing an information recording medium having a first read-only area recording a specified key management information, a second read-only area recording compressed data comprising said key management information compressed with a specified function according to a recording system different from that for said first read-only area, and a third read-only area recording encrypted content data resulting from encryption based on said key management information;

reading key management information from said first read-only area on said information recording medium and converting said key management information to compressed data by using a specified function;

reading compressed data from said second read-only area and comparing this compressed data with the compressed data obtained at said conversion;

when both match as a result of said comparison, generating a content key from said key management information by using its own device key; and

reading said encrypted content data from said third read-only area, decrypting said encrypted content data by using said generated content key, and outputting obtained content data.

15. An information recording medium comprising:

a first read-only area recording specified key management information;

a second read-only area recording compressed data comprising said key management information compressed with a specified function according to a recording system different from that for said first read-only area; and

a third read-only area for only once recording encrypted content data resulting from encryption based on said key management information.

16. The information recording medium according to claim 15, wherein said first read-only area is arranged in between said second read-only area and said third read-only area.

17. The recording apparatus for recording information on the information recording medium described in claim 15, comprising:

a compression circuit configured to convert key management information read from a first read-only area on said information recording medium to compressed data by using a specified function;

a comparison circuit configured to compare compressed data read from a second read-only area on said information recording medium with compressed data obtained in said compression circuit;

a key generation circuit configured to generate a content key from said key management information by using its own device key when a match is found as a result of comparison by said comparison circuit; and an encryption recording circuit configured to encrypt input content data by using a content key generated in said key generation circuit and record obtained encrypted content data onto said third read-only area.

18. The playback apparatus for playing information from the information recording medium described in claim 15, comprising:

a compression circuit configured to convert key management information read from a first read-only area on said information recording medium to compressed data by using a specified function;

a comparison circuit configured to compare compressed data read from a second read-only area on said information recording medium with compressed data obtained in said compression circuit;

a key generation circuit configured to generate a content key from said key management information by using its own device key when a match is found as a result of comparison by said comparison circuit; and

a decryption circuit configured to decrypt encrypted content data read from a third read-only area on said information recording medium by using a content key generated in said key generation circuit and output obtained content data.

19. An information recording medium comprising:

a first read-only area recording specified key management information;

a second read-only area recording compressed data comprising said key management information compressed with a specified function according to a recording system different from that for said first read-only area; and

a third read-only area recording encrypted content data resulting from encryption based on said key management information.

20. An information recording medium comprising:

a first read-only area recording specified key management information, wherein said key management information, after it is read, is used as compressed data converted with a specified function and is compared to compressed data in said second read-only area.

a second read-only area recording compressed data comprising said key management information compressed with a specified function according to a recording system different from that for said first read-only area; and

a third read-only area for recording encrypted content data based on said key management information when said comparison results in a match.